

# Zwei Probleme aus der Berechnungskomplexität

Inaugural-Dissertation  
zur Erlangung der Philosophischen Doktorwürde  
vorgelegt der  
Philosophischen Fakultät II  
der Universität Zürich

von  
WERNER HARTMANN  
aus Möriken AG

Begutachtet von Herrn Prof. Dr. V. Strassen

Zürich 1983  
Zentralstelle der Studentenschaft



# Zwei Probleme aus der Berechnungskomplexität

Inaugural-Dissertation  
zur Erlangung der Philosophischen Doktorwürde  
vorgelegt der  
Philosophischen Fakultät II  
der Universität Zürich

von  
WERNER HARTMANN  
aus Möriken AG

Begutachtet von Herrn Prof. Dr. V. Strassen

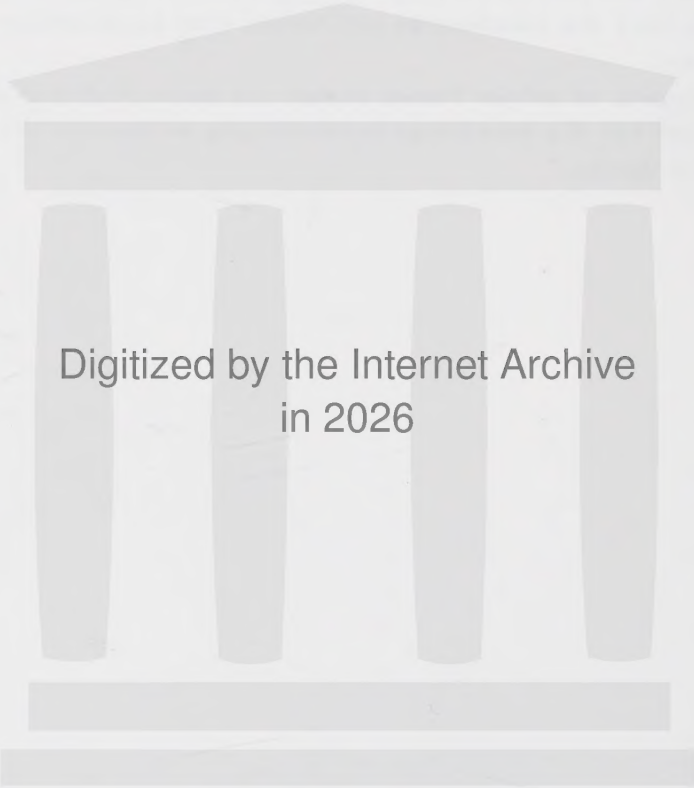
Zürich 1983  
Zentralstelle der Studentenschaft



### Vorbemerkung

Die folgende Arbeit besteht aus zwei Teilen. Im ersten Teil wird die Komplexität von Immanenten untersucht, im zweiten Teil die Komplexität von Moduln über assoziativen Algebren.

Die Anregung zu beiden Themen stammt von Herrn Prof.V.Strassen. Dafür und für die beständige Unterstützung möchte ich ihm herzlich danken.



Digitized by the Internet Archive  
in 2026

[https://archive.org/details/IA41507202\\_0011](https://archive.org/details/IA41507202_0011)

## 1. Teil

### UEBER DIE KOMPLEXITAET VON IMMANENTEN



## 1. Einleitung

Sei  $A = (a_{ij})$  eine  $n \times n$  Matrix. Die Permanente von  $A$  ist definiert als

$$\text{Perm } A = \sum_{\sigma} \prod_{i=1}^n a_{i, \sigma(i)} ,$$

wobei summiert wird über die  $n!$  Permutationen von  $\{1, \dots, n\}$ .

Im Gegensatz zur Determinante hat also jeder Summand ein positives Vorzeichen.

Sowohl die Permanente als auch die Determinante können als Spezialfälle von verallgemeinerten Matrixfunktionen aufgefasst werden. Sei  $\chi: S_n \rightarrow \mathbb{C}$  ein irreduzibler (komplexer) Charakter der symmetrischen Gruppe  $S_n$ .

$$d_{\chi}(A) = \sum_{\sigma \in S_n} \chi(\sigma) \prod_{i=1}^n a_{i, \sigma(i)}$$

heißt die zu  $\chi$  gehörige Immanente von  $A$ .

Ist  $\chi$  der identische bzw. der Signum-Charakter, so erhalten wir die Permanente bzw. Determinante.

Immanenten haben unter anderem die folgende algebraische Bedeutung:

Sei  $V$  ein komplexer Vektorraum der Dimension  $m$  mit einem Skalarprodukt  $(\cdot, \cdot)$ . Das  $n$ -fache Tensorprodukt  $V^{\otimes n}$  ist ein  $S_n$ -Modul vermöge

$$\sigma(v_1 \otimes \dots \otimes v_n) = v_{\sigma^{-1}(1)} \otimes \dots \otimes v_{\sigma^{-1}(n)} .$$

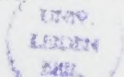
Seien  $\chi_1, \dots, \chi_s$  die irreduziblen Charaktere von  $S_n$ ,

$$(1) \quad V^{\otimes n} = \bigoplus_{i=1}^s V_{\chi_i}$$

die isotypische Zerlegung des  $S_n$ -Moduls  $V^{\otimes n}$  und

$$(2) \quad T_{\chi_i} = \frac{\chi_i(1)}{n!} \sum_{\sigma \in S_n} \chi_i(\sigma) \sigma : V^{\otimes n} \rightarrow V_{\chi_i}$$

die Projektion auf die zu  $\chi_i$  gehörende isotypische Komponente.



( , ) induziert ein Skalarprodukt auf  $V^n$  vermöge

$$(v_1 \otimes \dots \otimes v_n, w_1 \otimes \dots \otimes w_n) = \prod_{1 \leq i \leq n} (v_i, w_i)$$

und es gilt

$$(3) \quad (T_{X_i}(v_1 \otimes \dots \otimes v_n), T_{X_i}(w_1 \otimes \dots \otimes w_n)) = \frac{X_i(1)}{n!} d_{X_i}((v_\ell, w_k)_{\ell, k}).$$

(Für Einzelheiten siehe man z.B. [5].)

Abgesehen vom algebraischen Aspekt haben Immanente auch eine algorithmische Bedeutung. Trotz der Aehnlichkeit der algebraischen Ausdrücke sind die Determinante und die Permanente vom Gesichtspunkt der Berechnungskomplexität her gesehen zwei grundverschiedene Funktionen. Während es für die Berechnung der Determinante effiziente polynomiale Algorithmen gibt, brauchen alle bisher bekannten Methoden zur Auswertung der Permanente exponentielle Zeit. Der beste bekannte Algorithmus zur Auswertung der Permanente einer  $n \times n$  Matrix benötigt  $2^{n+O(\log n)}$  Schritte [7].

In [9] zeigt Valiant, dass die Berechnung der Permanente einer  $n \times n$   $\{0,1\}$ -Matrix NP-schwierig [2] ist. In [10] überträgt er dieses Resultat in die algebraische Sprache der  $p$ -definierbaren Familien von Polynomen über einem Körper  $k$  und zeigt, dass für  $\text{char } k \neq 2$  die Permanente in diesem Sinne vollständig ist. (In der gleichen Arbeit zeigt Valiant, dass auch die Determinante eine Universalitätseigenschaft hat: Jedes Polynom der Formelgrösse  $u$  ist eine Projektion der  $(u+2) \times (u+2)$  Determinante.)

Im folgenden untersuchen wir - im Sinne der Ostrowski-Zählung - die Komplexität von beliebigen Immanenten. Die Rekursionsformel für Charaktere von  $S_n$  liefert in trivialer Weise einen Algorithmus zur Berechnung einer zu einem beliebigen irreduziblen Charakter von  $S_n$  gehörigen Immanente mit Aufwand  $e^{O(n \log n)}$ .

Es stellt sich heraus, dass eine Klasse von der Determinante benachbarter Immanenten in polynomialer Zeit berechnet werden kann, während eine Klasse von der Permanente benachbarter Immanenten exponentielle Zeit benötigt, falls die Komplexität der Permanente exponentiell in  $n$  wächst. Dazwischen gibt es Immanenten, die zwar in subexponentieller Zeit, unter obiger Annahme aber nicht in polynomialer Zeit berechnet werden können.

## 2. Resultate

Im folgenden fassen wir  $\mathbb{C}[x_{11}, \dots, x_{nn}]$  als  $\mathbb{C}$ -Algebra über den Unbestimmten  $x_{11}, x_{12}, \dots, x_{nn}$  auf. Mit  $L(f)$  bezeichnen wir die minimale Anzahl nichtskalärer Multiplikationen, die zur Berechnung von  $f \in \mathbb{C}[x_{11}, \dots, x_{nn}]$  benötigt werden. Lineare Operationen wie Additionen, Subtraktionen und Skalarmultiplikationen betrachten wir als kostenlos. Dass wir Divisionen nicht zulassen, ist keine wesentliche Einschränkung, da Divisionen die Berechnung eines Polynoms vom Grad  $n$  höchstens um einen Faktor  $cn$  beschleunigen können für eine Konstante  $c$  [8].

Eine Partition  $\lambda$  von  $n$  ist eine Folge  $(\lambda_1, \dots, \lambda_s)$  von natürlichen Zahlen mit  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_s$ ,  $\lambda_s \neq 0$  und  $\lambda_1 + \dots + \lambda_s = n$ , kurz  $\lambda \vdash n$ . Oft schreiben wir anstelle von  $(\lambda_1, \dots, \lambda_s)$  auch  $(1^{\alpha_1}, \dots, n^{\alpha_n})$ , wo  $\alpha_i$  die Anzahl der  $\lambda_k$  mit  $\lambda_k = i$  bezeichnet.

Partitionen stellt man üblicherweise durch sogenannte Rahmen (Young Diagramme, Tableaux) dar. Der zu  $\lambda = (\lambda_1, \dots, \lambda_s)$  gehörende Rahmen besteht aus  $s$  Zeilen, die  $i$ -te Zeile enthält  $\lambda_i$  Felder. Beispiel: Der zu  $\lambda = (4, 3, 2, 1, 1)$  gehörende Rahmen ist in Figur 1 gezeichnet.



Fig. 1

Unter einem regulären Randstück  $r$  eines Rahmens versteht man eine Menge  $r$  von (via Kanten) zusammenhängenden rechtsunteren Randstücken, bei deren Wegnahme wieder ein Rahmen entsteht. Die zu einem so erhaltenen kleineren Rahmen gehörende Partition bezeichnen wir mit  $\lambda - r$ . Das Vorzeichen  $\text{sgn}(r)$  eines regulären Randstücks  $r$  ist  $+1$  bzw.  $-1$ , falls die Anzahl der vom Randstück getroffenen Zeilen des Rahmens ungerade bzw. gerade ist.

Zwischen den Partitionen von  $n$  und den irreduziblen (komplexen) Charakteren der symmetrischen Gruppe  $S_n$  besteht eine natürliche Bijektion. Ebenso werden die Konjugationsklassen von  $S_n$  durch die Partitionen von  $n$  beschrieben. Ist eine Partition  $\lambda \vdash n$  gegeben und bezeichnen wir mit  $\chi^\lambda$  den zugehörigen irreduziblen Charakter, so kann der Wert von  $\chi^\lambda$  auf einem Element der zur Partition  $\alpha \vdash n$  gehörenden Konjugationsklasse z.B. gemäss folgender Rekursionsformel berechnet werden (siehe z.B. [1]):

$$(4) \quad \chi^{(0)}(0) = 1$$

$$\chi^\lambda(1^{\alpha_1}, \dots, n^{\alpha_n}) = \sum_r \operatorname{sgn}(r) \chi^{\lambda-r}(1^{\alpha_1}, \dots, h^{\alpha_h-1}, \dots, n^{\alpha_n}),$$

wobei  $h \leq n$  beliebig gewählt ist mit  $\alpha_h > 0$  und sich die Summe über alle regulären Randstücke von  $\lambda$  der Länge  $h$  erstreckt.

Ist  $\chi: S_n \rightarrow \mathbb{C}$  eine beliebige Klassenfunktion, so bezeichnen wir mit

$$d_\chi = \sum_{\sigma \in S_n} \chi(\sigma) \prod_{i=1}^n x_{i, \sigma(i)} \in \mathbb{C}[x_{11}, \dots, x_{nn}]$$

die zu  $\chi$  gehörende verallgemeinerte Immanente.

Ist speziell  $\chi = \chi^\lambda$  ein irreduzibler Charakter von  $S_n$ , schreiben wir für die zu  $\chi^\lambda$  gehörende Immanente  $d_\chi$  kurz  $d_\lambda$ . Insbesondere ist also  $d_{(1^n)} =: \operatorname{Det}_n$  die  $n \times n$  Determinante,  $d_{(n)} =: \operatorname{Perm}_n$  die  $n \times n$  Permanente. Ferner setzen wir  $\operatorname{Perm}_0 = 1$ .

Unter Berücksichtigung einer Formel von Murnaghan-Gamba zur Berechnung der irreduziblen Charaktere von  $S_n$  [1, S.196-199] erhalten wir die folgende obere Schranke für die Komplexität von Immanenten.

Satz 1 Sei  $\lambda = (\lambda_1, \dots, \lambda_s)$  eine Partition von  $n$ .  
Dann gilt

$$(5) \quad L(d_\lambda) \leq n^{6(n-s)+4}.$$

Eine sorgfältigere Abschätzung liefert

$$L(d_\lambda) \leq n^{n-s+o(n-s)}.$$

Betrachtet man insbesondere eine Folge  $(\lambda_n)_{n \in \mathbb{N}}$  von Partitionen mit der Eigenschaft, dass sich die zugehörigen Rahmen mit wachsendem  $n$  (ab einem gewissen  $n$ ) rechts der ersten Spalte nicht verändern, so impliziert Satz 1, dass die zugehörigen Immanenten in polynomialer Zeit in  $n$  berechnet werden können. Ein typischer Vertreter dieser Klasse ist

$$\lambda = (2, 1^{n-2})$$

mit

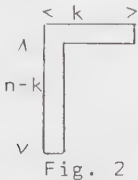
$$\chi^\lambda(\sigma) = \text{sgn}(\sigma) \cdot (\text{Anzahl Fixpunkte von } \sigma - 1)$$

für  $\sigma \in S_n$ .

Allgemeiner können wir sogenannte Winkelcharaktere  $\chi_k$  betrachten:

$$\chi_k = \chi^{(k, 1^{n-k})}, \quad k = 1, 2, \dots, n.$$

Den zugehörigen Rahmen zeigt Figur 2.



(5) liefert

$$L(d_{(k, 1^{n-k})}) \leq n^{6k}.$$

Insbesondere ist für konstantes  $k$   $d_{(k, 1^{n-k})}$  in polynomialer Zeit berechenbar. Satz 2 wird implizieren, dass für konstantes  $k$  der zu  $\chi_k$  konjugierte Charakter  $\chi'_k = \text{sgn} \cdot \chi_k$  eine Folge von Immanenten liefert, die mindestens so schwierig ist wie eine Folge von Permanenten vergleichbarer Grösse. Für eine Uebersicht über Winkelcharaktere und ihre Bedeutung siehe man [6].

Analog zum Vorgehen von Valiant [9] erhalten wir unter Berücksichtigung der kanonischen Bijektion zwischen Matrizen und vollständigen, gerichteten, gewichteten Graphen die folgende untere Schranke für die Komplexität von Immanenten.

Satz 2 Sei  $\lambda = (\lambda_1, \dots, \lambda_s)$  eine Partition von  $n$ ,  $\lambda \neq (n)$ .  
Dann gilt

$$(6) \quad L(d_\lambda) \geq L(\text{Perm}_{\left\lfloor \frac{\lambda_1 - \lambda_2}{\lambda_2 + s - 1} \right\rfloor}) .$$

Wendet man Satz 2 auf Winkelcharaktere an, so erhält man

$$L(d_{(n-k, 1^k)}) \geq L(\text{Perm}_{\left\lfloor \frac{n-k+1}{k+1} \right\rfloor}) .$$

Insbesondere würde also (für festes  $k$ ) ein in  $n$  polynomialer Algorithmus für  $d_{(n-k, 1^k)}$  einen polynomialen Algorithmus für  $\text{Perm}_n$  implizieren.

Unter Ausnützung der Rekursionsformel (4) für reguläre Randstücke maximaler Länge erhält man eine weitere untere Schranke.

Satz 3 Sei  $\lambda = (\lambda_1, \dots, \lambda_s)$  eine Partition von  $n$  und sei  $a = \max\{i \mid \lambda_i \geq i\}$ . Falls  $\lambda_{a+1} < a$  oder  $a = s$ , gilt

$$(7) \quad L(d_\lambda) \geq L(\text{Perm}_{\lambda_a - a + 1}) .$$

Satz 3 impliziert z.B. für Immanenten, die zu einem Doppelbalken, also einem Rahmen bestehend aus zwei gleichlangen Zeilen gehören,

$$L(d_{(n, n)}) \geq L(\text{Perm}_{n-1}) .$$

(Satz 3 liefert entsprechende Aussagen für eine ganze Klasse von der Permanente benachbarter Immanenten.)

Für Winkelcharaktere erhalten wir speziell noch

Satz 4 Für  $k \leq \left\lfloor \frac{n}{2} \right\rfloor$  gilt

$$(8) \quad L(d_{(k, 1^{n-k})}) \geq L(\text{Perm}_k) .$$

Unter der Annahme

$$L(\text{Perm}_n) \geq e^{cn} \quad \text{für eine Konstante } c > 0$$

liefert (5) zusammen mit (8) für  $k \leq \left\lfloor \frac{n}{2} \right\rfloor$

$$e^{ck} \leq L(d_{(k,1^{n-k})}) \leq e^{6 \log n k}.$$

Insbesondere würde z.B. für  $k = \left\lceil \log^2 n \right\rceil$  folgen

$$e^{c \log^2 n} \leq L(d_{(k,1^{n-k})}) \leq e^{c' \cdot \log^3 n}$$

für eine Konstante  $c'$ . D.h.  $d_{(k,1^{n-k})}$  wäre zwar in subexponentieller, nicht aber in polynomialer Zeit berechenbar.

### 3. Beweise

Das Konzept "Rahmen" kann verallgemeinert werden zu sogenannten "schiefen Rahmen". Seien  $\lambda = (\lambda_1, \dots, \lambda_s)$ ,  $\nu = (\nu_1, \dots, \nu_t)$  Partitionen mit  $\nu_i \leq \lambda_i$  für alle  $i$ . Der schiefe Rahmen  $\lambda/\nu$  entsteht aus dem zu  $\lambda$  gehörigen Rahmen durch Wegnahme des zu  $\nu$  gehörigen Rahmen.

Beispiel: Ist  $\lambda = (5, 4, 4, 2, 1)$  und  $\nu = (4, 2, 1, 1, 1)$ , so zeigt Figur 3 den schiefen Rahmen  $\lambda/\nu$ .



Fig. 3

Den schiefen Charakter  $\chi^{\lambda/\nu}$  definieren wir gemäss der Rekursionsformel (4) mit dem Unterschied, dass  $\chi^{\lambda/\nu}(0) = +1$  bzw.  $-1$ , falls  $t$  ungerade bzw. gerade ist.

Schiefe Rahmen und die zugehörigen Charaktere spielen in der Darstellungstheorie von  $S_n$  und damit in der Theorie der symmetrischen Funktionen bzw. im Schubertkalkül eine wichtige Rolle (siehe z.B. [3]).

Wir verwenden sie zur Formulierung einer Formel von Murnaghan-Gamba zur Berechnung der irreduziblen Charaktere von  $S_n$  (siehe [1], S.196-199). Diese Formel drückt die einzelnen Charaktere von  $S_n$  als Polynomfunktionen in den  $\alpha_i$ 's, der Anzahl Zykeln der Länge  $i$ , aus.

Lemma 1 Sei  $\mu = (\mu_1, \dots, \mu_r)$  eine Partition von  $n$ ,  $m = n - \mu_1$ . Dann gilt

$$(9) \quad \chi^\mu(1^{\alpha_1}, \dots, n^{\alpha_n}) =$$

$$\sum_{\substack{k_1, \dots, k_m \\ m-r+1 \leq \sum k_i \leq m}} \chi^{\mu/\nu_1, 1^{m-\sum k_i}}(1^{k_1}, \dots, m^{k_m}) \binom{\alpha_1}{k_1} \cdot \dots \cdot \binom{\alpha_m}{k_m}.$$

Beispiel: Sei  $\mu = (3, 2, 1)$ , also  $n = 6$ ,  $m = 3$ ,  $r = 3$ ,  $m-r+1 = 1$ .

Wir haben drei Fälle zu unterscheiden:

$\sum \ell k_\ell = 1$ : Der zu  $\mu/(3, 1^2)$  gehörende Rahmen hat die Gestalt



Also ist  $\chi^{\mu/(3, 1^2)}(1^1, 2^0, 3^0) = 1$ .

$\sum \ell k_\ell = 2$ : Der zu  $\mu/(3, 1)$  gehörende Rahmen hat die Gestalt



Also ist  $\chi^{\mu/(3, 1)}(1^2, 2^0, 3^0) = -2$

$\chi^{\mu/(3, 1)}(1^0, 2^1, 3^0) = 0$ .

$\sum \ell k_\ell = 3$ : Der zu  $\mu/(3)$  gehörende Rahmen hat die Gestalt



Also ist  $\chi^{\mu/(3)}(1^3, 2^0, 3^0) = 2$

$\chi^{\mu/(3)}(1^1, 2^1, 3^0) = 0$

$\chi^{\mu/(3)}(1^0, 2^0, 3^1) = -1$ .

Damit liefert (9)

$$\chi^{(3, 2, 1)}(1^{\alpha_1}, \dots, 6^{\alpha_6}) = \alpha_1 - 2 \binom{\alpha_1}{2} + 2 \binom{\alpha_1}{3} - \alpha_3.$$

Im Beweis des nächsten Lemmas geben wir einen Algorithmus zur Berechnung von  $d_x$  an für den Fall, dass  $x$  auf einem Element  $\sigma$  der zur Partition  $(1^{\alpha_1}, \dots, n^{\alpha_n})$  gehörenden Konjugationsklasse den Wert  $\text{sgn}(\sigma) \alpha_1^{i_1} \dots \alpha_m^{i_m}$  annimmt ( $m \leq n$ ). Anstelle von  $d_x$  schreiben wir

$d_{\text{sgn}} \alpha_1^{i_1} \dots \alpha_m^{i_m}$ . Wir benützen stillschweigend die kanonische Bijektion zwischen Matrizen und vollständigen, gerichteten, gewichteten Graphen:

Einer  $n \times n$  Matrix  $A = (a_{ij})$  ordnen wir den vollständigen, gerichteten Graphen mit  $n$  Punkten zu, dessen Kante vom Punkt  $i$  zum Punkt  $j$  das Gewicht  $a_{ij}$  hat. Unter einem  $(1,1)$ -Faktor eines  $n$ -punktigen Graphen verstehen wir einen  $n$ -punktigen Teilgraph bestehend aus lauter disjunkten Zyklen. Zwischen den  $(1,1)$ -Faktoren eines  $n$ -punktigen, vollständigen Graphen und den Permutationen aus  $S_n$  besteht also eine natürliche Bijektion.

## Lemma 2

$$(10) \quad L(d_{\text{sgn}} \alpha_1^{i_1} \dots \alpha_m^{i_m}) \leq L(\text{Det}_n) \prod_{1 \leq \ell \leq m} \left( \frac{n!}{(n-\ell)!} \right)^{i_\ell}.$$

Beweis: Wir führen neue Variable  $t_1^{(1)}, \dots, t_1^{(i_1)}, \dots, t_m^{(1)}, \dots, t_m^{(i_m)}$  ein. Mit  $\sigma_\ell^{(k)}$  bezeichnen wir einen Zykel der Länge  $\ell$  des zur Matrix  $(x_{ij})_{1 \leq i, j \leq n}$  gehörenden Graphen. Für alle Tupel  $(\sigma_1^{(1)}, \dots, \sigma_1^{(i_1)}, \dots, \sigma_m^{(1)}, \dots, \sigma_m^{(i_m)})$  definieren wir

$$A(\sigma_1^{(1)}, \dots, \sigma_m^{(i_m)}) \in M_n(\mathbb{Z}[x_{11}, \dots, x_{nn}, t_1^{(1)}, \dots, t_m^{(i_m)}])$$

vermöge

$$a_{ij} = x_{ij} \cdot \prod_{\ell, k} t_\ell^{(k)},$$

wobei das Produkt gebildet wird über alle Paare  $(\ell, k)$ , für die  $(i, j)$  eine Kante des Zyklus  $\sigma_\ell^{(k)}$  ist.

Mittels Koeffizientenvergleich verifiziert man

$$(11) \quad d_{\text{sgn} \cdot \alpha_1^{i_1} \dots \alpha_m^{i_m}} = \prod_{1 \leq \ell \leq m} \frac{1}{(\ell!)^{i_\ell}} \frac{\delta}{\delta t_1^{(1)}} \dots \left( \frac{\delta}{\delta t_m^{(i_m)}} \right)^m \sum \det A(\sigma_1^{(1)}, \dots, \sigma_m^{(i_m)}) ,$$

wobei summiert wird über alle Tupel  $(\sigma_1^{(1)}, \dots, \sigma_m^{(i_m)})$  für die  $\bigcup \sigma_\ell^{(k)}$  Teil eines  $(1,1)$ -Faktors ist.

Beachtet man, dass die Unbestimmten  $t_\ell^{(k)}$  für die Berechnung der rechten Seite von (11) nur eine symbolische Bedeutung haben, erhält man

$$\begin{aligned} L(d_{\text{sgn} \cdot \alpha_1^{i_1} \dots \alpha_m^{i_m}}) &\leq L(\text{Det}_n) \cdot \# \{ (\sigma_1^{(1)}, \dots, \sigma_m^{(i_m)}) \mid \bigcup \sigma_\ell^{(k)} \text{ ist Teil eines } (1,1)\text{-Faktors} \} \\ &\leq L(\text{Det}_n) \cdot \prod_{1 \leq \ell \leq m} \left( \frac{n!}{(n-\ell)!} \right)^{i_\ell} . \end{aligned}$$

Bemerkung 1 Analog erhalten wir

$$(12) \quad L(d_{\alpha_1^{i_1} \dots \alpha_m^{i_m}}) \leq L(\text{Perm}_n) \cdot \prod_{1 \leq \ell \leq m} \left( \frac{n!}{(n-\ell)!} \right)^{i_\ell} .$$

### Beweis von Satz 1

Sei  $\lambda = (\lambda_1, \dots, \lambda_s)$  eine Partition von  $n$ ,  $\mu = (\mu_1, \dots, \mu_r)$  die zu  $\lambda$  konjugierte Partition, also  $r = \lambda_1$ ,  $\mu_1 = s$  und  $x^\lambda = \text{sgn} \cdot x^\mu$ .

Mit Lemma 1 erhalten wir

$$(13) \quad d_\lambda = d_{\text{sgn} x^\mu} = \sum_{\substack{k_1, \dots, k_m \\ m-r+1 \leq \sum \ell k_\ell \leq m}} x^{\mu / (\mu_1, 1^{m-\sum \ell k_\ell})} (1^{k_1}, \dots, m^{k_m}) d_{\text{sgn} \left( \alpha_1 \right) \dots \left( \alpha_m \right)} ,$$

also

$$L(d_\lambda) \leq \sum_{\substack{k_1, \dots, k_m \\ \sum \ell k_\ell \leq m}} L(d_{\text{sgn}} \binom{\alpha_1}{k_1} \dots \binom{\alpha_m}{k_m}).$$

Bezeichnen wir mit  $p(i)$  die Anzahl Partitionen von  $i$  haben wir

$$(14) \quad L(d_\lambda) \leq \sum_{i \leq m} p(i) \cdot \max_{\substack{k_1, \dots, k_m \\ \sum \ell k_\ell \leq m}} L(d_{\text{sgn}} \binom{\alpha_1}{k_1} \dots \binom{\alpha_m}{k_m}).$$

Für festes  $(k_1, \dots, k_m)$  mit  $\sum \ell k_\ell \leq m$  ist  $\binom{\alpha_1}{k_1} \dots \binom{\alpha_m}{k_m}$  ein Polynom

in  $\alpha_1, \dots, \alpha_m$  vom Grad  $k_\ell$  in  $\alpha_\ell$  mit höchstens  $\prod_{1 \leq \ell \leq m} (k_\ell + 1)$  Monomen.

Wegen  $k_\ell \leq \frac{m}{\ell}$  für alle  $\ell$  ist

$$\prod_{1 \leq \ell \leq m} (k_\ell + 1) = \prod_{1 \leq \ell \leq m} \frac{m + \ell}{\ell} = \binom{2m}{m} \text{ und damit}$$

$$(15) \quad L(d_{\text{sgn}} \binom{\alpha_1}{k_1} \dots \binom{\alpha_m}{k_m}) \leq \binom{2m}{m} \cdot \max L(d_{\text{sgn}} \cdot \alpha_1^{i_1} \dots \alpha_m^{i_m}),$$

wobei das Maximum genommen wird über alle Tupel  $(i_1, \dots, i_m)$  mit

$$i_\ell \leq k_\ell.$$

Mit (10) erhalten wir

$$\begin{aligned} L(d_{\text{sgn}} \cdot \alpha_1^{i_1} \dots \alpha_m^{i_m}) &\leq L(\text{Det}_n) \cdot \prod_{1 \leq \ell \leq m} \left( \frac{n!}{(n-\ell)!} \right)^{k_\ell} \\ &\leq L(\text{Det}_n) \cdot \prod_{1 \leq \ell \leq m} n^{\ell k_\ell} \\ &\leq L(\text{Det}_n) \cdot n^m. \end{aligned}$$

Zusammenfassend ergibt sich

$$\begin{aligned} L(d_\lambda) &\leq \left( \sum_{i \leq m} p(i) \right) \binom{2m}{m} \cdot L(\text{Det}_n) \cdot n^m \\ &\leq (m+1) e^{3\sqrt{m}} 2^m n^3 n^m. \end{aligned}$$

Beachten wir  $m+1 \leq n$  und  $m = n-s$ , so folgt für  $n \geq 3$

$$L(d_\lambda) \leq n^{6m+4} = n^{6(n-s)+4}.$$

Eine sorgfältigere Abschätzung liefert

$$L(d_\lambda) \leq n^{n-s+o(n-s)}.$$

Bemerkung 2 Verfahren wir im obigen Beweis analog ohne zum konjugierten Charakter  $\chi^\mu$  überzugehen, erhalten wir zusammen mit Bemerkung 1

$$(16) \quad L(d_\lambda) \leq n^{6(n-\lambda_1)+1} \cdot L(\text{Perm}_n).$$

Für die Beweise der unteren Schranken benutzen wir wiederum die kanonische Bijektion zwischen vollständigen, gerichteten, gewichteten Graphen und Matrizen. Jeder Summand der Permanente einer Matrix entspricht dabei dem Produkt der Kantengewichte eines  $(1,1)$ -Faktors des entsprechenden Graphen.

#### Beweis von Satz 2

Sei  $\lambda = (\lambda_1, \dots, \lambda_s)$  eine Partition von  $n$ ,  $\lambda \neq (n)$ .

Es genügt eine Matrix  $A \in M_n(\{x_{11}, \dots, x_{nn}\} \cup \{0,1\})$  anzugeben mit

$$\text{Perm} \begin{bmatrix} \lambda_1 - \lambda_2 \\ \lambda_2 + s - 1 \end{bmatrix} = c \cdot d_\lambda(A), \quad c \in \mathbb{C}.$$

(denn  $L(d_\lambda) \geq L(d_\lambda(A))$ )

Seien  $m = \begin{bmatrix} \lambda_1 - \lambda_2 \\ \lambda_2 + s - 1 \end{bmatrix}$  und  $G$  der zur  $m \times m$  Matrix  $(x_{ij})$  gehörende Graph

mit  $m$  Punkten. Wir ersetzen jeden Punkt  $P_i$  von  $G$  durch einen Teilgraphen gemäss Figur 4, indem wir  $P_i$  in zwei Punkte  $P'_i$  und  $P''_i$  aufspalten und dazwischen  $\lambda_2 + s - 3$  durch mit 1 gewichtete Kanten verbundene Punkte einfügen.

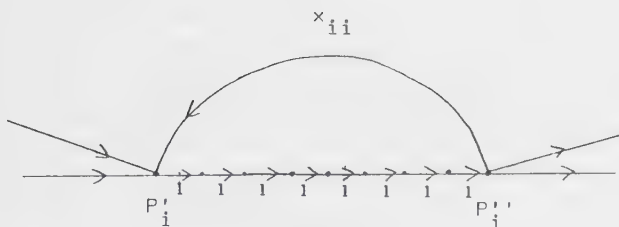


Fig. 4

Ferner erhält die Kante von  $P'_{i'}$  nach  $P'_i$  das Gewicht  $x_{ii}$ . In  $P_i$  eintretende bzw. austretende Kanten treten im neuen Graphen in  $P'_i$  ein bzw. in  $P'_{i'}$  aus.

Fügen wir nun noch  $n-m(\lambda_2+s-1)$  Punkte gemäss Figur 5 hinzu,



Fig. 5

vervollständigen wir den so erhaltenen Graphen und gewichten wir die dabei entstehenden Kanten mit 0, erhalten wir einen Graphen  $G'$  mit folgenden Eigenschaften:

- $G'$  hat  $n$  Punkte.
- Die  $\{1,1\}$ -Faktoren von  $G$  und  $G'$  mit nichtverschwindenden Produkten der Kantengewichte entsprechen sich bijektiv und die Produkte stimmen überein.
- Jeder  $\{1,1\}$ -Faktor von  $G'$ , der von einem  $\{1,1\}$ -Faktor von  $G$  herrührt, enthält  $n-m(\lambda_2+s-1)$  Zyklen der Länge 1.

Die restlichen Zyklen haben mindestens die Länge  $\lambda_2+s-1$ . Berücksichtigt man, dass reguläre Randstücke von  $\lambda$  der Länge  $\lambda_2+s-1$  oder mehr in der ersten Zeile beginnen und dass  $m(\lambda_2+s-1) \leq \lambda_1 - \lambda_2$  ist, so folgt für alle  $\sigma \in S_n$ , die von einem  $\{1,1\}$ -Faktor in  $G$  herrühren

$$\chi^\lambda(\sigma) = \chi^{(\lambda_1 - m(\lambda_2+s-1), \lambda_2, \dots, \lambda_s)}(1) = : c'$$

und damit

$$\text{Perm}_m = \frac{1}{c}, d_\lambda(A),$$

wo  $A$  die zu  $G'$  gehörende  $n \times n$  Matrix ist.

Zum Beweis von Satz 3 benützen wir

Lemma 3 Sei  $\lambda = (\lambda_1, \dots, \lambda_s)$  eine Partition von  $n$  und sei für alle  $t \geq 0$   $s_t = s - t - \#\{i \mid \lambda_i \leq t\}$ . Dann gilt

$$(17) \quad \forall a \ (0 \leq a \leq \max\{t \mid s_t > 0\}) \quad L(d_\lambda) \geq L(d_{\lambda\langle a \rangle}),$$

$$\text{wo } \lambda\langle a \rangle = (\lambda_{a+1}^{-a}, \lambda_{a+2}^{-a}, \dots, \lambda_{a+s_a}^{-a}).$$

Beweis: Durch Induktion nach  $a$ .

Wegen  $\lambda\langle 0 \rangle = (\lambda_1, \dots, \lambda_s)$  genügt es zu zeigen

$$L(d_{\lambda\langle a \rangle}) \geq L(d_{\lambda\langle a+1 \rangle}).$$

Wie im Beweis von Satz 2 zeigen wir, dass es eine Matrix  $A$  aus  $M_{n\langle a \rangle}(\{x_{11}, \dots, x_{nn}\} \cup \{0, 1\})$  gibt mit

$$d_{\lambda\langle a+1 \rangle} = c \cdot d_{\lambda\langle a \rangle}(A),$$

wobei  $\lambda\langle a \rangle \vdash n\langle a \rangle$  und  $c \in \mathbb{C}$ .

Sei  $A$  die  $n \times n$  Matrix

$$\left( \begin{array}{c|c} x_{ij} & 0 \\ \hline 0 & \begin{array}{c} 1 \\ \diagdown \quad \diagup \\ 1 \quad 0 \end{array} \end{array} \right)$$

bestehend aus einem Block  $(x_{ij})$  und dem einem Zykel der Länge  $\lambda_{a+1}^{-a+s_a}-1$  entsprechenden zweiten Block.  $\lambda_{a+1}^{-a+s_a}-1$  ist gerade die Länge des maximalen regulären Randstückes  $r$  von  $\lambda\langle a \rangle$  und wegen (4) gilt

$$d_{\lambda\langle a \rangle}(A) = (-1)^{s_a+1} d_{\lambda\langle a \rangle} - r.$$

Bleibt noch zu zeigen

$$\lambda\langle a \rangle - r = \lambda\langle a+1 \rangle.$$

Klar ist

$$\lambda \langle a \rangle^{-r} = (\lambda_{a+2}^{-a-1}, \lambda_{a+3}^{-a-1}, \dots, \lambda_{a+b}^{-a-1}).$$

Also genügt es noch  $b = s_{a+1} + 1$  zu zeigen.

Wir haben

$$\begin{aligned} b &= s_a - \#(i | \lambda_{a+i}^{-a-1}) \\ &= s_a - \#(i | \lambda_{a+i}^{-a+1}) \\ &= s_a - \#(i | \lambda_i \leq a) - \#(i | \lambda_{a+i}^{-a+1}) \\ &= s_a - \#(i | \lambda_i \leq a+1). \end{aligned}$$

Bei der letzten Gleichheit haben wir benutzt, dass für  $i \leq a$   $\lambda_i = a+1$  impliziert  $s_{a+1} < 0$ , Widerspruch zur Voraussetzung  $s_{a+1} > 0$ .

### Beweis von Satz 3

Wir haben für  $a = \max\{i | \lambda_i \geq i\}$

$$s_{a-1} = s - (a-1) - \#(i | \lambda_i \leq a-1).$$

Wegen  $\lambda_{a+1} < a$  oder  $a = s$  folgt

$$\#(i | \lambda_i \leq a-1) = s - a,$$

also

$$s_{a-1} = 1.$$

(17) liefert somit

$$L(d_\lambda) \geq L(d_{\lambda \langle a-1 \rangle}),$$

wobei  $\lambda \langle a-1 \rangle = (\lambda_a^{-a+1})$ , also  $d_{\lambda \langle a-1 \rangle} = \text{Perm}_{\lambda_a^{-a+1}}$ .

### Beweis von Satz 4

Wegen  $k \leq \lfloor \frac{n}{2} \rfloor$  beginnt das einzige reguläre Randstück der Länge  $n-k$  in der zweiten Zeile des zur Partition  $(k, 1^{n-k})$  gehörenden Rahmens. Analog zum Induktionsschritt im Beweis von Lemma 3 erhalten wir eine  $n \times n$  Matrix  $A$  so, dass

$$d_{(k, 1^{n-k})}(A) = (-1)^{n-k+1} d_{(k)} = (-1)^{n-k+1} \text{Perm}_k.$$

#### 4. Ergänzungen

Zur Berechnung der Determinante besitzt man mit der Gauss-elimination einen effizienten Algorithmus. Dabei benützt man, dass die Determinante einer Matrix verschwindet, wenn zwei Zeilen oder Spalten der Matrix gleich sind oder wenn der Rang nicht maximal ist. Der folgende Satz verallgemeinert diese Aussagen auf beliebige Immanente.

##### Satz (R.Merris [4])

Sei  $\lambda = (\lambda_1, \dots, \lambda_s)$  eine Partition von  $n$ . Dann gilt für  $A \in M_n(\mathbb{C})$ :

- (i) Hat  $A$  mehr als  $\lambda_1$  gleiche Zeilen oder Spalten, so ist  $d_\lambda(A) = 0$ .
- (ii) Ist der Rang von  $A$  kleiner  $s$ , so ist  $d_\lambda(A) = 0$ .

Ob aufgrund dieser Eigenschaften die Gausselimination auf beliebige Immanente übertragen werden kann ist unklar.

## Literatur

- [1] H.Boerner, Darstellungen von Gruppen, Springer Berlin(1967).
- [2] S.A.Cook, The complexity of theorem proving procedures, Proc.3rd ACM Symp. on Theory of Computing(1971)151-158.
- [3] M.Hamermesh, Group theory, Addison-Wesley, Reading, 1962.
- [4] R.Merris, On vanishing decomposable symmetrized tensors, Linear and Multilinear Algebra 5 (1977)79-86.
- [5] R.Merris, Recent advances in symmetry classes of tensors, Linear and Multilinear Algebra 7 (1979)317-328.
- [6] R.Merris, Single-Hook characters and Hamiltonian Circuits, preprint.
- [7] H.J.Ryser, Combinatorial Mathematics, Carus Math.Monograph no.14 (1963) 24ff.
- [8] V.Strassen, Vermeidung von Divisionen, J.Reine Angew.Math. 264 (1973)184-202.
- [9] L.G.Valiant, The complexity of computing the permanent, Theor.Comput.Sci. 8 (1979)189-201.
- [10] L.G.Valiant, Completeness classes in algebra, Proc. 11th ACM Symp. on Theory of Computing (1979)249-261.



## 2. Teil

UEBER DIE KOMPLEXITAET VON MODULN UEBER ASSOZIATIVEN ALGEBREN



## 1. Einleitung

Sei  $k$  ein unendlicher Körper,  $A$  eine  $n$ -dimensionale assoziative  $k$ -Algebra (mit 1) und  $M$  ein  $m$ -dimensionaler (Links-)  $A$ -Modul. Sei  $e_1, \dots, e_n$  eine Basis des Vektorraumes  $A$ ,  $f_1, \dots, f_m$  eine Basis des Vektorraumes  $M$ ,

$$e_i \cdot f_j = \sum_{\ell=1}^m \tau_{ij\ell} f_\ell$$

mit  $\tau_{ij\ell} \in k$ . Dann ist

$$\left( \sum_{i=1}^n \xi_i e_i \right) \cdot \left( \sum_{j=1}^m \eta_j f_j \right) = \sum_{\ell=1}^m \left( \sum_{i,j=1}^{n,m} \tau_{ij\ell} \xi_i \eta_j \right) f_\ell.$$

Seien  $x_1, \dots, x_n, y_1, \dots, y_m$  Unbestimmte über  $k$ .

Im folgenden benützen wir das Ostrowskische Berechnungsmodell für  $k(x_1, \dots, x_n, y_1, \dots, y_m)$ , d.h. wir betrachten lineare Operationen wie Additionen, Subtraktionen und Skalarmultiplikationen als kostenlos und minimalisieren die Anzahl nichtskalärer Multiplikationen/ Divisionen.

Definition Die Komplexität des  $A$ -Moduls  $M$  ist

$$L(A, M) = L\left(\left\{ \sum_{i,j=1}^{n,m} \tau_{ij\ell} x_i y_j \mid 1 \leq \ell \leq m \right\}\right).$$

$L(A, M)$  hängt nicht von der gewählten Basis ab.

In [1] haben Alder-Strassen eine allgemeine untere Schranke für die Komplexität der Multiplikation in einer Algebra  $A$  bewiesen:

$$L(A, A) \geq 2 \dim A - \text{Anzahl maximaler zweiseitiger Ideale von } A.$$

Wir beweisen eine Verallgemeinerung dieser unteren Schranke auf beliebige  $A$ -Moduln  $M$ .

## 2. Resultate

Wir reduzieren das Problem in verschiedenen Schritten auf Moduln über einfachen Algebren. Für die dazu benützten Tatsachen über Moduln und Algebren siehe man z.B. [3], Kapitel 2 und 3.

Zuerst beachten wir, dass isomorphe  $A$ -Moduln die gleiche Komplexität haben. Ferner gilt: Ist  $M$  ein  $A$ -Modul,  $f: A' \rightarrow A$  ein Algebrenmorphismus, so kann  $M$  auch als  $A'$ -Modul aufgefasst werden. Für  $f$  surjektiv gilt dabei

$$L(A', M) = L(A, M).$$

(  $L(A', M) \leq L(A, M)$  ist trivial. Da  $f: A' \rightarrow A$  als surjektiver Morphismus von  $k$ -Vektorräumen einen Schnitt hat, folgt auch  $L(A', M) \geq L(A, M)$ . )

Insbesondere ist also  $L(A', M) = L(A, M)$ , falls  $f: A' \rightarrow A$  ein Isomorphismus ist.

Sei  $\text{ann}(M) = \{a \in A \mid aM = 0\}$  der Annihilator von  $M$ .  $\text{ann}(M)$  ist ein zweiseitiges Ideal in  $A$ ,  $M$  aufgefasst als  $A/\text{ann}(M)$  ist treu und wir haben

$$L(A, M) = L(A/\text{ann}(M), M) \quad .$$

Im folgenden können wir uns deshalb auf treue  $A$ -Moduln beschränken.

Betrachten wir einen  $A$ -Modul  $M$  und einen  $B$ -Modul  $N$ , so sind  $M$  bzw.  $N$  vermöge der Projektionen  $A \times B \rightarrow A$  bzw.  $A \times B \rightarrow B$   $A \times B$ -Moduln.  $M \otimes N$  kann somit als  $A \times B$ -Modul aufgefasst werden. Umgekehrt ist jeder  $A \times B$ -Modul  $P$  von der Form  $M \otimes N$ , wo  $M$  ein  $A$ -Modul und  $N$  ein  $B$ -Modul ist. (nämlich  $M = (1, 0)P$  und  $N = (0, 1)P$  )

Analog zum Vorgehen von Alder-Strassen reduzieren wir das Problem nun auf halbeinfache Algebren. Mit  $\text{rad}A$  bezeichnen wir das Radikal von  $A$ , mit  $\text{rad}M$  dasjenige von  $M$ . Es ist  $\text{rad}M = \text{rad}A \cdot M$  und  $M/\text{rad}M$  kann als  $A/\text{rad}A$ -Modul aufgefasst werden.

Satz 1 Sei  $M$  ein treuer  $A$ -Modul. Dann gilt

$$L(A, M) \geq L(A/\text{rad}A, M/\text{rad}M) + \dim(\text{rad}A) + \dim(\text{rad}M).$$

$A/\text{rad}A$  ist halbeinfach, also nach dem Struktursatz von Wedderburn isomorph einem direkten Produkt von vollen Matrixalgebren  $K_i^{n_i \times n_i}$  über  $k$ -Divisionsalgebren  $K_i$ . Die Moduln eines solchen Faktors  $K^{n \times n}$  sind bis auf Isomorphie von der Form  $K^{n \times m}$ . (Skalarmultiplikation=Matrixmultiplikation)

Mehrfache Anwendung des nächsten Satzes liefert deshalb untere Schranken für Moduln über halbeinfachen Algebren.

Satz 2 Sei  $K$  eine  $k$ -Divisionsalgebra,  $\dim_K K = \lambda$ ,  $B$  eine beliebige Algebra,  $N$  ein beliebiger  $B$ -Modul. Dann gilt für  $n, m \geq 1$

$$L(K^{n \times n} \times B, K^{n \times m} \otimes N) \geq f(n, m, \lambda) + L(B, N)$$

wobei

$$f(n, 1, \lambda) = \lambda n^2 + (\lambda - 1)n$$

$$f(n, m, \lambda) = \lambda \cdot \max\{n^2, nm - m + n\} + \lambda nm - 1 \quad \text{falls } n, m > 1$$

$$f(1, m, \lambda) = (2\lambda - 1)m.$$

Obiger Satz lässt sich auch koordinatenfrei formulieren:

Sei  $A$  eine einfache Algebra,  $M \neq 0$  ein  $A$ -Modul. Sei  $E$  einfacher Untermodul von  $M$ ,  $F$  einfacher Untermodul des  $\text{End}_A M$ -Moduls  $M$  und  $K^{\text{op}}$  die Endomorphismenalgebra von  $E$ . Sei ferner  $B$  eine beliebige Algebra,  $N$  ein beliebiger  $B$ -Modul. Dann gilt:

$$L(A \times B, M \otimes N) \geq \dim_K A + \dim_K M - \dim_K M + L(B, N) \quad \text{falls } \dim_K F = 1$$

$$L(A \times B, M \otimes N) \geq \max\{\dim_K A, \dim_K M - (\dim_K F - \dim_K E)\} + \dim_K M - 1 + L(B, N) \quad \text{falls } \dim_K E, \dim_K F > 1$$

$$L(A \times B, M \otimes N) \geq 2\dim_K M - \dim_K M + L(B, N) \quad \text{falls } \dim_K E = 1.$$

Mit Hilfe dieser Sätze erhalten wir die nachfolgenden Korollare.

Korollar 1 (A. Alder, V. Strassen [1])

Sei  $A$  eine beliebige Algebra. Dann gilt

$$L(A, A) \geq 2\dim A - s,$$

wo  $s$  die Anzahl maximaler zweiseitiger Ideale von  $A$  ist.

Beweis: A aufgefasst als A-Modul ist treu. Satz 1 liefert

$$L(A, A) \geq L(A/\text{rad}A, A/\text{rad}A) + 2\dim(\text{rad}A).$$

$A/\text{rad}A$  ist isomorph einem direkten Produkt von einfachen Algebren, etwa

$$A \simeq \prod_{i=1}^s K_i^{n_i \times n_i}, \quad \dim_k K_i = \lambda_i.$$

s stimmt mit der Anzahl maximaler zweiseitiger Ideale von A überein. Mehrfaches Anwenden von Satz 2 mit  $n=m$  liefert somit

$$\begin{aligned} L(A/\text{rad}A, A/\text{rad}A) &\geq \sum_{n_i=1} (2\lambda_i - 1) + \sum_{n_i \geq 1} (2\lambda_i n_i^2 - 1) \\ &= 2\dim(A/\text{rad}A) - s. \end{aligned}$$

Zusammen erhalten wir

$$L(A, A) \geq 2\dim A - s.$$

Die untere Schranke für  $n=1$  liefert zusammen mit der bekannten oberen Schranke das nächste Korollar.

Korollar 2 (L.Auslander, S.Winograd [2])

Sei K eine k-Divisionsalgebra,  $\dim_k K = \lambda$ . Dann gilt

$$L(K, K^m) \geq (2\lambda - 1)m.$$

Für die Multiplikation von Matrizen über k erhalten wir

Korollar 3

$$L(k^{n \times n}, k^{n \times m}) \geq \begin{cases} n^2 & \text{falls } m=1 \\ \max\{n^2 + nm - 1, 2nm + n - m - 1\} & \text{falls } m > 1 \end{cases}$$

Für  $m=1$  bzw.  $m=n$  entspricht dies den bekannten Schranken.

Für  $n=2$  erhalten wir insbesondere:

Korollar 4

$$L(k^{2 \times 2}, k^{2 \times m}) \geq 3m + 1.$$

Bekannt ist

$$L(k^{2 \times 2}, k^{2 \times m}) \leq 3m + 2$$

(S. Winograd, [5]).

Wegen  $L(k^{2 \times 2}, k^{2 \times 2}) = 7$  ist zumindest für  $m=2$  die untere Schranke scharf.

Sei  $D_{2n}$  die Diedergruppe der Ordnung  $2n$ ,  $\mathbb{C}[D_{2n}]$  ihre Gruppenalgebra über  $k=\mathbb{C}$ . Unter Verwendung der Charaktertheorie erhält man für ungerades  $n$

$$\mathbb{C}[D_{2n}] \simeq \mathbb{C}^2 \times (\mathbb{C}^{2 \times 2})^{(n-1)/2},$$

für gerades  $n$

$$\mathbb{C}[D_{2n}] \simeq \mathbb{C}^4 \times (\mathbb{C}^{2 \times 2})^{n/2-1},$$

d.h. die irreduziblen Darstellungen von  $D_{2n}$  sind entweder ein- oder zweidimensional.

Sei  $M$  ein beliebiger  $\mathbb{C}[D_{2n}]$ -Modul. Betrachten wir eine direkte Summenzerlegung von  $M$  in einfache Moduln und bezeichnen wir mit  $s$  die Anzahl der dabei auftretenden eindimensionalen Moduln und mit  $t$  die Anzahl der isotypischen Komponenten, die zu zweidimensionalen Darstellungen gehören, so erhalten wir die folgende untere Schranke.

Korollar 5  $L(\mathbb{C}[D_{2n}], M) \geq s + \frac{3}{2}(\dim M - s) + t.$

Beweis: Sei  $M$  ein treuer  $\mathbb{C}^{\ell} \times (\mathbb{C}^{2 \times 2})^t$ -Modul,  $M'$  eine isotypische Komponente,  $M = M' \oplus M''$  und  $s$  wie oben.

Gehört  $M'$  zu einer eindimensionalen Darstellung, so liefert

Satz 2 mit  $n=\lambda=1$  und  $m=\dim M'$

$$L(\mathbb{C}^{\ell} \times (\mathbb{C}^{2 \times 2})^t, M) \geq \dim M' + L(\mathbb{C}^{\ell-1} \times (\mathbb{C}^{2 \times 2})^t, M'').$$

Gehört  $M'$  zu einer zweidimensionalen Darstellung, liefert Satz 2 mit  $n=2$ ,  $\lambda=1$  und  $m=\frac{1}{2} \dim M'$

$$\begin{aligned} L(\mathbb{C}^{\ell} \times (\mathbb{C}^{2 \times 2})^t, M) &\geq 3m+1 + L(\mathbb{C}^{\ell} \times (\mathbb{C}^{2 \times 2})^{t-1}, M'') \\ &= \frac{3}{2} \dim M' + 1 + L(\mathbb{C}^{\ell} \times (\mathbb{C}^{2 \times 2})^{t-1}, M''). \end{aligned}$$

Beachten wir, dass  $s$  die Summe ist der Dimensionen der isotypischen Komponenten zu eindimensionalen Darstellungen,  $\dim M - s$  diejenige der isotypischen Komponenten zu zweidimensionalen Darstellungen erhalten wir induktiv

$$L(\mathbb{C}^{\ell \times (\mathbb{C}^{2 \times 2})^t}, M) \geq s + \frac{3}{2}(\dim M - s) + t.$$

Analog erhalten wir unter Verwendung von  $L(k^{2 \times 2}, k^{2 \times m}) \leq 3m + 2$  als obere Schranke

$$L(\mathbb{C}[D_{2n}], M) \leq s + \frac{3}{2}(\dim M - s) + 2t.$$

Im nächsten Korollar bestimmen wir die Komplexität von  $k[x]/(f)$ -Moduln für den Fall, dass  $f$  quadratfrei ist. In diesem Fall ist  $k[x]/(f)$  halbeinfach. Bezeichnen wir mit  $s$  die Anzahl einfacher Moduln in einer direkten Summenzerlegung von  $M$ , so erhalten wir das folgende Korollar.

Korollar 6 Sei  $f \in k[x]$  quadratfrei. Dann gilt

$$L(k[x]/(f), M) = 2\dim M - s.$$

Beweis: Sei  $f = p_1 \dots p_r$  eine Primfaktorzerlegung.

Wegen

$$k[x]/(f) \simeq \prod_{i=1}^r K_i$$

mit  $K_i \simeq k[x]/(p_i)$  ist  $M$  bis auf Isomorphie eine direkte Summe von  $K_i$ -Moduln  $K_i^{s_i}$ ,  $i=1, \dots, r$ . Dabei ist  $s = s_1 + \dots + s_r$ .

Wir zeigen durch Induktion nach  $\ell \leq r$

$$L\left(\prod_{i=1}^{\ell} K_i, \bigoplus_{i=1}^{\ell} K_i^{s_i}\right) \geq 2 \sum_{i=1}^{\ell} \dim K_i s_i - (s_1 + \dots + s_{\ell}).$$

(Insbesondere also  $L\left(\prod_{i=1}^r K_i, M\right) \geq 2\dim M - s$ .)

Der Induktionsanfang ist trivial. Satz 2 mit  $n=1$ ,  $\lambda = \dim K_{\ell}$  und  $m = s_{\ell}$  liefert

$$L\left(\prod_{i=1}^{\ell} K_i, \bigoplus_{i=1}^{\ell} K_i^{s_i}\right) \geq (2\dim K_{\ell} - 1)s_{\ell} + L\left(\prod_{i=1}^{\ell-1} K_i, \bigoplus_{i=1}^{\ell-1} K_i^{s_i}\right)$$

$$\geq 2 \cdot \sum_{i=1}^{\ell} \dim_k K_i \cdot s_i = (s_1 + \dots + s_{\ell}). \quad (\text{Induktionsvoraussetzung})$$

Durch eine entsprechende Induktion zeigt man unter Verwendung von Korollar 2, dass die obere Schranke mit der unteren übereinstimmt.

Bezeichnet  $C_n$  die zyklische Gruppe der Ordnung  $n$  und beachtet man, dass

$$k[C_n] \cong k[x]/(x^n - 1)$$

und dass  $x^n - 1$  quadratfrei ist, falls  $\text{char } k \nmid n$ , so beschreibt also Korollar 6 insbesondere die Komplexität beliebiger  $k[C_n]$ -Moduln für  $\text{char } k \nmid n$ .

### 3. Beweise

Die Multiplikation  $A \times M \rightarrow M$  ist eine bilineare Abbildung. Wir betrachten die Berechnungskomplexität von etwas allgemeineren Abbildungen, nämlich homogenen quadratischen Abbildungen.

Definition Seien  $E, W$  endlichdimensionale  $k$ -Vektorräume mit Basen  $e_1, \dots, e_n$  bzw.  $f_1, \dots, f_m$ . Eine Abbildung  $h: E \rightarrow W$  heisst quadratisch, wenn es quadratische Formen  $h_1, \dots, h_m$  in  $k[x_1, \dots, x_n]$  gibt, so dass für alle  $\xi_1, \dots, \xi_n \in k$

$$h\left(\sum_{i=1}^n \xi_i e_i\right) = \sum_{\ell=1}^m h_{\ell}(\xi_1, \dots, \xi_n) f_{\ell}.$$

$L(h) = L(h_1, \dots, h_m)$  nennen wir die Komplexität von  $h$ .

Der Begriff "quadratische Abbildung" und  $L(h)$  hängen nicht von der gewählten Basis ab. Sind ferner  $\Phi: E' \rightarrow E$ ,  $\Psi: W \rightarrow W'$  lineare Abbildungen, so ist auch  $\Psi \circ h \circ \Phi$  quadratisch und es gilt

$$(1) \quad L(h) \geq L(\Psi \circ h \circ \Phi).$$

Satz Sei  $h: E \rightarrow W$  quadratisch. Dann gilt

$L(h) \leq r$  genau, wenn es  $u_{\rho}, v_{\rho} \in E^*$ ,  $w_{\rho} \in W$  ( $\rho=1, \dots, r$ ) gibt, sodass für alle  $x \in E$

$$h(x) = \sum_{\rho=1}^r u_{\rho}(x) v_{\rho}(x) w_{\rho},$$

wobei  $E^*$  den Dualraum von  $E$  bezeichnet.

Der Beweis dieses Satzes beruht auf der Tatsache, dass quadratische Formen optimal ohne Divisionen berechnet werden können. (siehe [4])

Das folgende technische Lemma, welches die in [1] verwandte Methode zusammenfasst, verdanke ich einer Mitteilung von Herrn Strassen.

Lemma 1  $A, B$  und  $W$  seien endlichdimensionale  $k$ -Vektorräume,  
 $h: A \times B \rightarrow W$  eine bilineare Abbildung, die wir als Multiplikation  
 schreiben:

Sei für alle  $a \in A, b \in B$

$$(2) \quad a \cdot b = \sum_{\rho=1}^r u_{\rho}(a, b) v_{\rho}(a, b) w_{\rho}$$

mit  $u_{\rho}, v_{\rho} \in (A \times B)^*$ ,  $w_{\rho} \in W$  und seien  $X \subset A, Y' \subset Y \subset B, P \subset W$  lineare  
 Teilräume, sodass die  $u_{\rho}$  mit  $w_{\rho} \notin P$  die Punkte von  $X \times Y'$  trennen,  
 also den Dualraum von  $X \times Y'$  erzeugen. Dann gilt

Entweder

(i) Nach Vertauschen gewisser  $u_{\rho}$  mit  $v_{\rho}$  trennen die  $u_{\rho}$  mit  
 $w_{\rho} \notin P$  die Punkte von  $X \times Y$ .

oder

(ii) Es gibt  $y \in Y \setminus Y'$  mit  $Ay \subseteq P + X \cdot Y$ .

(Analog seitenvertauscht)

Beweis: Wir nehmen an, (i) sei verletzt. Bei Permutation von  
 Summanden in (2) und Vertauschen gewisser  $u_{\rho}$  mit  $v_{\rho}$  können wir  
 o.B.d.A. annehmen

$$w_1, \dots, w_p \in P, \quad w_{p+1}, \dots, w_r \notin P$$

$u_{p+1}, \dots, u_r$  trennen die Punkte von  $X \times Y'$

$u_{p+1}, \dots, u_q$  linear unabhängig auf  $X \times Y$

$u_{q+1}, \dots, u_r, v_{q+1}, \dots, v_r$  linear abhängig von  $u_{p+1}, \dots, u_q$

als Linearformen auf  $X \times Y$

$u_{p+1}, \dots, u_r$  trennen die Punkte von  $X \times Y$  nicht.

Insbesondere trennen  $u_{p+1}, \dots, u_q$  die Punkte von  $X \times Y'$ , nicht aber  
 von  $X \times Y$ .

D.h. es gibt  $x \in X, y \in Y \setminus Y'$  mit  $u_{p+1}(x, y) = \dots = u_q(x, y) = 0$ .

Damit gilt auch

$$u_{q+1}(x, y) = \dots = u_r(x, y) = 0$$

$$v_{q+1}(x, y) = \dots = v_r(x, y) = 0.$$

Sind  $a \in A$ ,  $b \in B$  beliebig, so finden wir wegen der linearen Unabhängigkeit von  $u_{p+1}, \dots, u_q$  auf  $X \times Y$   $s \in X$ ,  $t \in Y$  mit

$$\forall p \quad (p+1 \leq p \leq q) \quad u_p(a, b) = -u_p(s, t)$$

$$\text{also } u_{p+1}(a+s, b+t) = \dots = u_q(a+s, b+t) = 0.$$

Damit erhalten wir

$$\begin{aligned} (a+s)y + x(b+t+y) &= (a+s+x)(b+t+y) - (a+s)(b+t) = \\ &= \sum_{p=1}^r (u_p(a+s, b+t) + u_p(x, y))(v_p(a+s, b+t) + v_p(x, y))w_p - \\ &= \sum_{p=1}^r u_p(a+s, b+t)v_p(a+s, b+t)w_p = \\ &= \sum_{p=1}^r (u_p(a+s, b+t)v_p(x, y) + u_p(x, y)v_p(a+s, b+t) + u_p(x, y)v_p(x, y))w_p. \end{aligned}$$

Wegen

$$u_{p+1}(x, y) = \dots = u_r(x, y) = 0$$

$$u_{p+1}(a+s, b+t) = \dots = u_q(a+s, b+t) = 0$$

$$v_{q+1}(x, y) = \dots = v_r(x, y) = 0$$

folgt

$$\begin{aligned} (a+s)y + x(b+t+y) &= \sum_{p=1}^p (u_p(a+s, b+t)v_p(x, y) + u_p(x, y)v_p(a+s, b+t) \\ &\quad + u_p(x, y)v_p(x, y))w_p \in P. \end{aligned}$$

Setzen wir  $b=0$  folgt

$$ay + xt + (s+x)y \in P$$

also

$$Ay \subset P + X \cdot Y.$$

### Beweis von Satz 1

Sei  $L(A, M) = r$ . Dann gibt es  $u_\rho, v_\rho \in (A \times M)^*$ ,  $w_\rho \in M$  so, dass

$$(3) \quad \forall a \in A, x \in M \quad ax = \sum_{\rho=1}^r u_\rho(a, x) v_\rho(a, x) w_\rho.$$

Es genügt, eine Darstellung (3) zu finden mit der zusätzlichen Eigenschaft, dass

(4)  $u_1, \dots, u_r$  die Punkte von  $\text{rad} A \times \text{rad} M$  trennen.

Denn sei  $q_1 = \dim(\text{rad} A)$ ,  $q_2 = \dim(\text{rad} M)$  und gelte (4). O.B.d.A. können wir dann annehmen

$u_1, \dots, u_{q_1+q_2}$  linear unabhängig auf  $\text{rad} A \times \text{rad} M$ .

Sei  $E = \{u_1 = \dots = u_{q_1+q_2} = 0\} \subset A \times M$ .

Dann ist  $E \cap (\text{rad} A \times \text{rad} M) = 0$ .

Sei  $h: E \rightarrow M$  die Restriktion der Multiplikation  $A \times M \rightarrow M$ .

$h$  ist quadratisch und

$$L(h) \leq r - (q_1 + q_2).$$

$$(\text{denn } h(a, x) = \sum_{\rho=q_1+q_2+1}^r u_\rho(a, x) v_\rho(a, x) w_\rho)$$

Sei  $\mu$  bzw.  $\mu'$  die Multiplikation  $A \times M \rightarrow M$  bzw.  $A/\text{rad} A \times M/\text{rad} M \rightarrow M/\text{rad} M$ .

Das kommutative Diagramm

$$\begin{array}{ccc} A \times M & \xrightarrow{\mu} & M \\ \downarrow & & \downarrow \\ A/\text{rad} A \times M/\text{rad} M & \xrightarrow{\mu'} & M/\text{rad} M \end{array}$$

liefert (vermöge Restriktion) ein kommutatives Diagramm

$$\begin{array}{ccc} E & \xrightarrow{h} & M \\ \downarrow \alpha & & \downarrow \\ A/\text{rad} A \times M/\text{rad} M & \xrightarrow{\mu'} & M/\text{rad} M \end{array}.$$

Wegen  $E \cap (\text{rad} A \times \text{rad} M) = 0$  ist  $\alpha$  ein Isomorphismus und es folgt

$$\begin{aligned} L(A/\text{rad} A, M/\text{rad} M) &= L(\mu') \leq L(h) \leq r - (q_1 + q_2) \\ &= L(A, M) - \dim(\text{rad} A) - \dim(\text{rad} M) \end{aligned}$$

Also genügt es eine Darstellung (3) mit der Eigenschaft (4) zu haben:

Nach Vertauschen gewisser  $u_\rho$  mit  $v_\rho$  trennen  $u_1, \dots, u_r$  die Punkte von  $\text{rad} A \times 0$ .

Andernfalls liefert Lemma 1 mit  $P=0$ ,  $X'=0$ ,  $X=\text{rad} A$ ,  $Y=0$  ein  $a \in \text{rad} A$ ,  $a \neq 0$  mit  $aM=0$ , also da  $M$  treu ist einen Widerspruch.

Da  $\text{rad} A$  nilpotent ist, gibt es ein  $k$  mit  $(\text{rad} A)^k = 0$ . Durch umgekehrte Induktion nach  $i$ ,  $1 \leq i \leq k$ , zeigen wir, dass nach Vertauschen gewisser  $u_\rho$  mit  $v_\rho$   $u_1, \dots, u_r$  auch die Punkte von  $\text{rad} A \times (\text{rad} A)^i M$ , insbesondere also auch von  $\text{rad} A \times \text{rad} M$  trennen.

Der Induktionsanfang  $i=k$  wurde oben erledigt.

Könnten wir nicht induktiv von  $i$  auf  $i-1$  schliessen, würde Lemma 1 mit  $P=0$ ,  $X=\text{rad} A$ ,  $Y'=(\text{rad} A)^i M$ ,  $Y=(\text{rad} A)^{i-1} M$  ein  $x \in (\text{rad} A)^{i-1} M \setminus (\text{rad} A)^i M$  liefern, so dass

$$Ax \in \text{rad} A \cdot (\text{rad} A)^{i-1} M = (\text{rad} A)^i M$$

also  $x \in (\text{rad} A)^i M$ , ein Widerspruch.

Zum Beweis von Satz 2 benötigen wir noch das folgende technische Lemma.

Lemma 2 Sei  $K$  eine endlichdimensionale  $k$ -Divisionsalgebra,  $\dim_k K = \lambda$ ,  $w_1, \dots, w_{\lambda n}$  eine  $k$ -Basis des  $K$ -Moduls  $K^n$ . Dann gilt mit  $t = n(\lambda - 1)$

$\exists (i_1, \dots, i_t) \quad 1 \leq i_1 < \dots < i_t \leq \lambda n$  so dass  $P = kw_{i_1} + \dots + kw_{i_t}$

keine  $K$ -Gerade enthält.

Beweis: Wir zeigen durch Induktion nach  $\ell < t$ :

$\exists (i_1, \dots, i_\ell) \quad 1 \leq i_1 < \dots < i_\ell \leq \lambda n$  so dass  $P = kw_{i_1} + \dots + kw_{i_\ell}$   
keine  $K$ -Gerade enthält.

Der Induktionsanfang ist trivial.

Für den Induktionsschritt dürfen wir o.B.d.A. annehmen, dass

$P = kw_1 + \dots + kw_{\ell-1}$  keine K-Gerade enthält. Es genügt zu zeigen, dass es  $j \geq \ell$  gibt so, dass  $P + kw_j$  keine K-Gerade enthält.

Nehmen wir an, dass  $P + kw_j$  für alle  $j \geq \ell$  eine K-Gerade  $g_j$  enthält, folgt wegen  $\lambda_{n-\ell+1} \geq \lambda_{n-t+1} = n+1$  und  $\dim_K g_j = \lambda$ , dass

$g_\ell + \dots + g_{\lambda_n}$  nicht direkt sein kann. O.B.d.A. ist also

$$g_{\lambda_n} \cap (g_\ell + \dots + g_{\lambda_n-1}) \neq 0,$$

also  $g_{\lambda_n} \subset g_\ell + \dots + g_{\lambda_n-1}$

und damit

$$g_{\lambda_n} \subset (P + kw_{\lambda_n}) \cap (P + kw_\ell + \dots + kw_{\lambda_n-1}) = P,$$

d.h. P enthält eine K-Gerade, Widerspruch.

## Beweis von Satz 2

Sei  $L(K^{n \times n} \times B, K^{n \times m} \otimes N) = r$ . Dann gibt es  $u_\rho, v_\rho$  aus  $((K^{n \times n} \times B) \times (K^{n \times m} \otimes N))^*$ ,  $w_\rho \in K^{n \times m} \otimes N$  mit

$$\forall (a,b) \in K^{n \times n} \times B, \forall (x,y) \in K^{n \times m} \otimes N \quad (ax, by) = \sum_{\rho=1}^r u_\rho(a,b;x,y) v_\rho(a,b;x,y) w_\rho.$$

Im folgenden bezeichnen wir  $K^{n \times n}$ -Untermodule von  $K^{n \times m}$  als Linksmoduln,  $\text{End}_{K^{n \times n}} K^{n \times m}$ -Untermodule von  $K^{n \times m}$  als Rechtsmoduln.

### Fall $m=1$ :

Indem wir jedem  $\mu \in K^{op}$  die Rechtsmultiplikation in  $K^n$  mit  $\mu$  als Endomorphismus zuordnen, haben wir wegen  $m=1$   $K^{n \times m} = K^n$  und

$$\text{End}_{K^{n \times n}} K^n \simeq K^{op}.$$

Ferner erzeugen  $w_1, \dots, w_r$   $K^n \otimes N$ , also ist  $r \geq \lambda_n$  und o.B.d.A.

können wir annehmen, dass  $w_1, \dots, w_{\lambda_n}$  k-linear unabhängig sind und dass mit

$$W = kw_1 + \dots + kw_{\lambda_n}$$

gilt

$$W \cap N = 0.$$

(Man wähle  $w_1, \dots, w_{\lambda_n}$  so, dass die Projektionen auf  $K^n$  linear-unabhängig sind.)

Insbesondere haben wir dann

$$K^n \otimes N = W \otimes N.$$

Sei  $w_\rho = w'_\rho \otimes w''_\rho$ ,  $w'_\rho \in K^n$ ,  $w''_\rho \in N$  ( $1 \leq \rho \leq r$ ).

$w'_1, \dots, w'_{\lambda n}$  bilden eine  $k$ -Basis von  $K^n$ . Sei  $t = (\lambda - 1)n$ .

Gemäss Lemma 2 (angewendet auf  $\text{End}_{K^{n \times n}} K^n = K^{0 \times 0}$ ) dürfen wir o.B.d.A. annehmen

$$P' = kw'_1 + \dots + kw'_t \subset K^n$$

enthält keine  $\text{End}_{K^{n \times n}} K^n$ -Gerade, also überhaupt keinen Rechtsuntermodul  $\neq 0$ .

Sei  $P = kw_1 + \dots + kw_t$ .

Zeigen: Nach Vertauschen gewisser  $u_\rho$  mit  $v_\rho$  trennen die  $u_\rho$  mit  $\rho > t$  die Punkte von  $(K^{n \times n} \times 0) \times 0$ .

(Insbesondere ist dann  $r \geq \lambda n^2 + t = \lambda n^2 + (\lambda - 1)n$ .)

Andernfalls liefert Lemma 1 mit obigem  $P$ ,  $X' = 0 \times 0$ ,  $X = K^{n \times n} \times 0$ ,  $Y = 0$  ein  $a \in K^{n \times n}$ ,  $a \neq 0$  mit

$$(a, 0) \cdot (K^n \otimes N) = aK^n \subset P,$$

also  $aK^n \subset P'$ .

$aK^n$  ist ein Rechtsuntermodul von  $K^n$ , also ist

$$aK^n = 0,$$

d.h.  $a$  ist im Annihilator des  $K^{n \times n}$ -Moduls  $K^n$ , Widerspruch.

O.B.d.A. dürfen wir also annehmen, dass die Restriktionen von  $u_{t+1}, \dots, u_{t+\lambda n^2}$  eine Basis von  $((K^{n \times n} \times 0) \times 0)^*$  bilden.

Sind  $b \in B$ ,  $y \in N$  beliebig, finden wir deshalb ein eindeutig bestimmtes  $a \in K^{n \times n}$  so, dass

$$(5) \quad \forall \rho \quad (t+1 \leq \rho \leq t+\lambda n^2) \quad u_\rho(a, 0; 0, 0) = -u_\rho(0, b; 0, y).$$

Damit ist

$$a0 \otimes by = by = \sum_{\rho=1}^t u_\rho(a, b; 0, y) v_\rho(a, b; 0, y) w_\rho + \sum_{\rho=t+\lambda n^2+1}^r u_\rho(a, b; 0, y) v_\rho(a, b; 0, y) w_\rho.$$

Bezeichnen wir mit  $\sigma: W \otimes N \rightarrow N$  die Projektion längs  $W$ , so folgt also

$$by = \sum_{\rho=t+\lambda n^2+1}^r u_{\rho}(a,b;0,y) v_{\rho}(a,b;0,y) \sigma(w_{\rho}) .$$

(5) beschreibt ein lineares Gleichungssystem für  $a$ . Deshalb können die  $u_{\rho}$  und  $v_{\rho}$  in obiger Darstellung als Linearformen auf  $B \times N$  aufgefasst werden.

Somit haben wir

$$L(B,N) \leq r - (t + \lambda n^2) .$$

Fall  $n=1$ :

Analog zum Fall  $m=1$  können wir o.B.d.A. annehmen, dass  $w_1, \dots, w_{\lambda m}$   $k$ -linearunabhängig sind und dass mit

$$W = kw_1 + \dots + kw_{\lambda m}$$

gilt

$$W \cap N = 0 ,$$

also

$$K^m \otimes N = W \otimes N .$$

In Analogie zum Fall  $m=1$  dürfen wir diesmal mit  $t=(\lambda-1)m$  o.B.d.A. annehmen, dass

$$P' = kw'_1 + \dots + kw'_t \subset K^m$$

keinen Linksuntermodul  $\neq 0$  enthält.

Sei  $P = kw_1 + \dots + kw_t$ .

Zeigen: Nach Vertauschen gewisser  $u_{\rho}$  mit  $v_{\rho}$  trennen die  $u_{\rho}$  mit  $\rho > t$  die Punkte von  $0 \times K^m$ .

(Insbesondere ist dann  $r \geq \lambda m + t = (2\lambda - 1)m$ .)

Andernfalls liefert Lemma 1 ein  $x \in K^m$ ,  $x \neq 0$  mit

$$(K \times B)(x, 0) = Kx \subset P$$

also

$$Kx \subset P' .$$

$Kx$  ist ein Linksuntermodul von  $K^m$ , also ist

$$Kx = 0 ,$$

d.h.  $x=0$ , Widerspruch.

O.B.d.A. dürfen wir also annehmen, dass die Restriktionen von  $u_{t+1}, \dots, u_{t+\lambda m}$  eine Basis von  $(0 \times K^m)^*$  bilden. Sind  $b \in B$ ,  $y \in N$  beliebig, finden wir deshalb analog zum Fall  $m=1$  ein eindeutig bestimmtes  $x \in K^m$  so, dass

$$u_{t+1}(0, b; x, y) = \dots = u_{t+\lambda m}(0, b; x, y) = 0.$$

Bezeichnen wir mit  $\sigma: W \otimes N \longrightarrow N$  die Projektion längs  $W$ , so folgt also analog zum Fall  $m=1$

$$by = \sum_{\rho=t+\lambda m+1}^r u_{\rho}(0, b; x, y) v_{\rho}(0, b; x, y) \sigma(w_{\rho})$$

und somit

$$l(B, N) \leq r - (t + \lambda m).$$

Fall  $n \geq m \geq 1$ :

$$E = \begin{bmatrix} K & 0 & . & . & . & 0 \\ . & . & & & & . \\ . & . & & & & . \\ . & . & & & & . \\ . & . & & & & . \\ . & . & & & & . \\ K & 0 & . & . & . & 0 \end{bmatrix}$$

ist einfacher Linksuntermodul von  $K^{n \times m}$ . Sei

$$t = \text{codim}_K E - 1 = \lambda n(m-1) - 1.$$

Wiederum können wir o.B.d.A. annehmen, dass

$$w_1, \dots, w_{t+1} \text{ k-linearunabhängig sind}$$

und dass mit

$$W = kw_1 + \dots + kw_{t+1}$$

gilt

$$W \cap (E \otimes N) = 0$$

insbesondere also mit  $P = kw_1 + \dots + kw_t$

$$(6) \quad P \cap (E \otimes N) = 0.$$

$P + (E \otimes N)$  ist eine Hyperebene in  $K^{n \times m} \otimes N$ .

Damit ist

$$R = \{a \in K^{n \times n} \mid (a, 1)(K^{n \times m} \otimes N) \subset P + (E \otimes N)\}$$

ein echtes Rechtsideal in  $K^{n \times n}$ .

In drei Schritten zeigen wir, dass nach jeweiligem Vertauschen gewisser  $u_\rho$  mit  $v_\rho$  folgendes gilt:

(7)  $u_\rho$  mit  $\rho > t$  trennen die Punkte von  $(K^{n \times n} \times 0) \times E$

Schritt 1: Die  $u_\rho$  mit  $\rho > t$  trennen die Punkte von  $(R \times 0) \times 0$ .  
Andernfalls liefert Lemma 1 mit obigem  $P$ ,  $X' = 0 \times 0$ ,  $X = R \times 0$ ,  $Y = 0$  ein  $a \in R$ ,  $a \neq 0$  mit

$$(a, 0) \cdot (K^{n \times m} \oplus N) \subset P$$

also

$$aK^{n \times m} \subset P.$$

$aK^{n \times m}$  ist Rechtsmodul.

(6) impliziert

$$aK^{n \times m} \cap E = 0,$$

also  $aK^{n \times m} = 0$ , also  $a = 0$ , Widerspruch.

Schritt 2: Die  $u_\rho$  mit  $\rho > t$  trennen die Punkte von  $(R \times 0) \times E$ .

Andernfalls liefert Lemma 1 mit  $X = R \times 0$ ,  $Y' = 0$ ,  $Y = E$

ein  $x \in E$ ,  $x \neq 0$  mit

$$(K^{n \times n} \times B) \cdot x \subset P + RE.$$

Aber  $K^{n \times n} \cdot x = E$ , also

$$E \subset P + RE.$$

Wegen  $Re \subset E$  und (6) folgt

$$E \subset RE,$$

Widerspruch.

Schritt 3: Die  $u_\rho$  mit  $\rho > t$  trennen die Punkte von  $(K^{n \times n} \times 0) \times E$ .

Andernfalls liefert Lemma 1 mit  $X' = R \times 0$ ,  $X = K^{n \times n} \times 0$ ,  $Y = E$

ein  $a \in K^{n \times n} \setminus R$  mit

$$(a, 0) \cdot (K^{n \times m} \oplus N) \subset P + E,$$

also  $a \in R$ , nach Definition von  $R$ , Widerspruch.

Wir haben somit (7) gezeigt und dürfen o.B.d.A. annehmen, dass die Restriktionen von

$$u_{t+1}, \dots, u_{t'} \quad (t' = t + \lambda n^2 + \lambda n)$$

eine Basis von  $((K^{n \times n} \times 0) \times E)^*$  bilden.

Entsprechend den früheren Fällen finden wir zu  $b \in B$ ,  $y \in N$  beliebig eindeutig bestimmte  $a \in K^{n \times n}$ ,  $e \in E$  mit

$$u_{t+1}(a, b; e, y) = \dots = u_{t'}(a, b; e, y) = 0,$$

also

$$ae \otimes by = \sum_{\rho=1}^t u_{\rho}(a, b; e, y) v_{\rho}(a, b; e, y) w + \sum_{\rho=t'+1}^r u_{\rho}(a, b; e, y) v_{\rho}(a, b; e, y) w$$

Bezeichnet  $\sigma: W \otimes E \otimes N \longrightarrow N$  die Projektion längs  $W \otimes E$ , so folgt wegen  $ae \in E$

$$by = \sum_{\rho=t'+1}^r u_{\rho}(a, b; e, y) v_{\rho}(a, b; e, y) \sigma(w_{\rho}).$$

Wiederum können wir die  $u_{\rho}$  und  $v_{\rho}$  in obiger Darstellung als Linearformen auf  $B \times N$  auffassen.

Somit haben wir

$$L(B, N) \leq r - t' = r - \lambda n^2 - \lambda nm + 1.$$

Fall  $m \geq n \geq 1$ :

$$F = \begin{bmatrix} K & . & . & . & . & . & . & . & K \\ 0 & . & . & . & . & . & . & . & 0 \\ . & & & & & & & & . \\ . & & & & & & & & . \\ . & & & & & & & & . \\ 0 & . & . & . & . & . & . & . & 0 \end{bmatrix}$$

ist einfacher Rechtsuntermodul von  $K^{n \times m}$ .

Der Beweis verläuft analog zum Fall  $n \geq m \geq 1$ .

Sei  $t = \text{codim}_K F = \lambda(n-1)m - 1$

O.B.d.A. können wir annehmen, dass

$$w_1, \dots, w_{t+1} \text{ k-linearunabhängig sind}$$

und dass mit

$$W = kw_1 + \dots + kw_{t+1}$$

gilt

$$W \cap (F \otimes N) = 0.$$

Insbesondere gilt mit  $P = kw_1 + \dots + kw_t$

$$(8) \quad P \cap (F \oplus N) = 0.$$

$P + (F \oplus N)$  ist eine Hyperebene in  $K^{n \times m}_{\oplus N}$ .

Damit ist

$$L = \{x \in K^{n \times m} \mid (K^{n \times n} \times B) \cdot x \subset P + (F \oplus N)\}$$

ein echter Linksmodul in  $K^{n \times m}$ .

Sei

$$I = \begin{bmatrix} K & . & . & . & . & K \\ 0 & . & . & . & . & 0 \\ . & & & & & . \\ . & & & & & . \\ . & & & & & . \\ 0 & . & . & . & . & 0 \end{bmatrix} \subset K^{n \times n}.$$

In drei Schritten zeigen wir, dass nach jeweiligem Vertauschen gewisser  $u_\rho$  mit  $v_\rho$  folgendes gilt:

$$(9) \quad u_\rho \text{ mit } \rho > t \text{ trennen die Punkte von } (I \times 0) \times K^{n \times m}.$$

Schritt 1: Die  $u_\rho$  mit  $\rho > t$  trennen die Punkte von  $0 \times L$ .

Andernfalls liefert Lemma 1 ein  $x \in L$ ,  $x \neq 0$  mit

$$(K^{n \times n} \times B) \cdot x \subset P.$$

$K^{n \times n} \cdot x$  ist Linksmodul.

(8) impliziert

$$K^{n \times n} \cdot x \cap F = 0,$$

also  $K^{n \times n} \cdot x = 0$ , Widerspruch.

Schritt 2: Die  $u_\rho$  mit  $\rho > t$  trennen die Punkte von  $(I \times 0) \times L$ .

Andernfalls liefert Lemma 1 ein  $a \in I$ ,  $a \neq 0$  mit

$$(a, 0) \cdot (K^{n \times m}_{\oplus N}) \subset P + IL.$$

Aber  $aK^{n \times m} = F$ , also

$$F \subset P + IL.$$

Wegen  $IL \subset F$  und (8) folgt

$$F \subset IL$$

also

$$F \subset L$$

im Widerspruch zu  $L \subset K^{n \times m}$  echter Linksmodul.

Schritt 3: Die  $u_\rho$  mit  $\rho > t$  trennen die Punkte von  $(I \times 0) \times K^{n \times m}$ :  
Andernfalls liefert Lemma 1 ein  $x \in K^{n \times m} \setminus L$

$$(K^{n \times n} \times B) \cdot x \subset P + IK^{n \times m}.$$

Wegen  $IK^{n \times m} = F$  folgt

$$(K^{n \times n} \times B) \cdot x \subset P + F,$$

also  $x \in L$  nach Definition von  $L$ , Widerspruch.

Analog zum Fall  $n \geq m \geq 1$  erhalten wir schliesslich

$$\begin{aligned} L(B, N) &\leq r - t - \lambda n - \lambda nm \\ &= r - 2\lambda nm + \lambda(m - n) + 1. \end{aligned}$$

Literatur

- [1] A.Alder and V.Strassen, On the algorithmic complexity of associative algebras, Theoret.Comput.Sci.15(1981)201-211.
- [2] L.Auslander and S.Winograd, The multiplicative complexity of certain semi-linear systems defined by polynomials, Advances in Appl.Math.1(1980)257-299.
- [3] R.S.Pierce, Associative Algebras (Springer Verlag, New York, 1982).
- [4] V.Strassen, Vermeidung von Divisionen, J.Reine Angew. Math.264(1973)184-202.
- [5] S.Winograd, A new algorithm for inner product, IEEE Trans. Computers 17(1968)693-694.



## Curriculum Vitae

Am 23. Januar 1953 wurde ich, Werner Hartmann, in Meilen ZH geboren. Ich bin Bürger von Möriken AG. Nach dem Besuch der Primarschule in Schlieren besuchte ich das Realgymnasium Rämibühl in Zürich, wo ich 1972 die Maturität Typus B erhielt. Anschliessend studierte ich an der Universität Zürich Mathematik mit den Nebenfächern experimentelle und theoretische Physik. Dort und an der Eidgenössischen Technischen Hochschule besuchte ich Vorlesungen und Seminare u.a. bei den Dozenten Baur, Hill, Karrer, Keller, Kriszten, Kündig, Irminger, Meyer, Neuenschwander, Niederer, Specker, Steiner, Stammbach, Stoss, Strassen, Straumann, Strebel und Wirth. 1978 legte ich meine Diplomprüfung in Mathematik und obigen Nebenfächern ab. Von 1978-1982 war ich Assistent am Seminar für Angewandte Mathematik der Universität Zürich. Die vorliegende Arbeit entstand unter der Leitung von Herrn Prof. Dr. V. Strassen.





